# WEST Search History

DATE: Monday, November 24, 2003

| Set Name side by side | Query | Hit Count | Set Name result set |
|---|---|---|---|
| *DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=ADJ* | | | |
| L9 | L1 and "AES" | 2 | L9 |
| L8 | L1 same "AES" | 1 | L8 |
| L7 | L1 and (s-box or p-box) | 1 | L7 |
| L6 | L1 same (s-box or p-box) | 1 | L6 |
| L5 | L1 and (encrypt$3 or encipher$3) | 4 | L5 |
| L4 | L1 and ("data encryption standard" or "DES") | 44 | L4 |
| L3 | L1 same ("data encryption standard" or "DES") | 1 | L3 |
| L2 | L1 same (encrypt$3 or encipher$3) | 3 | L2 |
| L1 | (alu or "arithmetic logic unit") with (permut$5 or substitut$3) | 168 | L1 |

END OF SEARCH HISTORY

## Search Results

Search Results for: **[(arithmetic logic unit AND permutation AND substitution)]**
Found **4** of **123,929 searched.**

### Search within Results



**Sort by:** **Title** **Publication** **Publication Date** **Score** Binder

**Results 1 - 4 of 4** **short listing**

**1** New techniques and approaches: An end-to-end approach to globally scalable programmable networking 77%
Micah Beck , Terry Moore , James S. Plank
**Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture** August 2003
The three fundamental resources underlying Information Technology are bandwidth, storage, and computation. The goal of wide area infrastructure is to provision these resources to enable applications within a community. The end-to-end principles provide a scalable approach to the architecture of the shared services on which these applications depend. As a prime example, IP and the Internet resulted from the application of these principles to bandwidth resources. A similar application to storage r ...

**2** Three ECL designs for microprogrammable Writable Control Stores 77%
J. F. McDonald , R. Harris , J. Sustman
**Conference record of the 6th annual workshop on Microprogramming** September 1973
Three designs are presented for extremely fast microprogrammed timing and control sequencers driven by Writable Control Stores. These designs have been put forth with a view towards utilizing existing or impending developments in the field of Emitter Coupled Logic (ECL). One of the designs is directly applicable to an existing ECL minicomputer architecture (that of the Digital Scientific META-4). The other two are more conjectural. One of these modules has a parts cost of roughly only &doll ...

**3** Session 7: rendering: Shear-image order ray casting volume rendering 77%
Yin Wu , Vishal Bhatia , Hugh Lauer , Larry Seiler
**Proceedings of the 2003 symposium on Interactive 3D graphics** April 2003
This paper describes shear-image order ray casting, a new method for volume rendering. This method renders sampled data in three dimensions with image quality equivalent to the best of ray-per-pixel volume rendering algorithms (full image order), while at the same time retaining computational complexity and spatial coherence near

to that of the fastest known algorithm (shear-warp). In shear-image order, as in shear-warp, the volume data set is resampled along slices parallel to a face of the vol ...

**4** Session 4: Optimal organizations for pipelined hierarchical memories 77%

Gianfranco Bilardi , Kattamuri Ekanadham , Pratap Pattnaik

**Proceedings of the fourteenth annual ACM symposium on Parallel algorithms and architectures** August 2002

In a recent paper (SPAA'01), we have established that the Pipelined Hierarchical Random Access Machine (PH-RAM) is a powerful model of computation, where most of the memory latency can be hidden by concurrency of accesses. In the present work, we explore the physical feasibility of PH-RAMs.A pipelined hierarchical memory of size $S$ is characterized by two metrics: the access function a(&khgr;), denoting the time required by an access to location $x$, and the pipeline period $p(S)$, denoti ...

**Results 1 - 4 of 4** **short listing**

Your search matched **15** of **987057** documents.

A maximum of **15** results are displayed, **15** to a page, sorted by **Relevance** in **descending** order.
You may refine your search by editing the current search expression or entering a new one the text box.
Then click **Search Again**.

des<and>pipeline processing Search Again

**Results:**
Journal or Magazine = **JNL** Conference = **CNF** Standard = **STD**

1 **PIMM1, an image processing ASIC based on mathematical morpholog**
*Klein, J.C.; Peyrard, R.;*
ASIC Seminar and Exhibit, 1989. Proceedings., Second Annual IEEE , 25-28 Sep 1989
Page(s): P7 -1/1-4

[Abstract] [PDF Full-Text (312 KB)] **IEEE CNF**

2 **On the construction of very large integer multipliers**
*Hotz, G.; Molitor, P.; Zimmer, W.;*
Euro ASIC '91 , 27-31 May 1991
Page(s): 266 -269

[Abstract] [PDF Full-Text (224 KB)] **IEEE CNF**

3 **Near Shannon limit error-correcting coding and decoding: Turbo-code**
*Berrou, C.; Glavieux, A.; Thitimajshima, P.;*
Communications, 1993. ICC 93. Geneva. Technical Program, Conference Record International Conference on , Volume: 2 , 23-26 May 1993
Page(s): 1064 -1070 vol.2

[Abstract] [PDF Full-Text (492 KB)] **IEEE CNF**

4 **Practical experiences with the SPARXIL co-processor**
*Koch, A.; Golze, U.;*
Signals, Systems & Computers, 1997. Conference Record of the Thirty-First Asil Conference on , Volume: 1 , 2-5 Nov. 1997

Page(s): 394 -398 vol.1

[Abstract] [PDF Full-Text (664 KB)] **IEEE CNF**

5 **Rapid prototype of a fast data encryption standard with integrity processing for cryptographic applications**
*Guendouz, H.; Bouaziz, S.;*
Circuits and Systems, 1998. ISCAS '98. Proceedings of the 1998 IEEE Internatio Symposium on , Volume: 6 , 31 May-3 June 1998
Page(s): 434 -437 vol.6

[Abstract] [PDF Full-Text (248 KB)] **IEEE CNF**

6 **Cryptographic processor architectures for DES algorithm**
*Korkishko, T.; Melnyk, A.;*
AFRICON, 1999 IEEE , Volume: 1 , 28 Sept.-1 Oct. 1999
Page(s): 175 -180 vol.1

[Abstract] [PDF Full-Text (492 KB)] **IEEE CNF**

7 **A fully pipelined, 700 MBytes/s DES encryption core**
*Kim, I.; Steele, S.; Koller, J.G.;*
VLSI, 1999. Proceedings. Ninth Great Lakes Symposium on , 4-6 March 1999
Page(s): 386 -387

[Abstract] [PDF Full-Text (32 KB)] **IEEE CNF**

8 **High performance DES encryption in Virtex™ FPGAs using JBits™**
*Patterson, C.;*
Field-Programmable Custom Computing Machines, 2000 IEEE Symposium on , 1 April 2000
Page(s): 113 -121

[Abstract] [PDF Full-Text (712 KB)] **IEEE CNF**

9 **A high performance FPGA implementation of DES**
*McLoone, M.; McCanny, J.V.;*
Signal Processing Systems, 2000. SiPS 2000. 2000 IEEE Workshop on , 11-13 O 2000
Page(s): 374 -383

[Abstract] [PDF Full-Text (380 KB)] **IEEE CNF**

10 **Implementation of pipelined data encryption standard (DES) using A CPLD**
*Teo Pock Chueng; Yusoff, Z.M.; Sha'ameri, A.Z.;*
TENCON 2000. Proceedings , Volume: 3 , 24-27 Sept. 2000
Page(s): 17 -21 vol.3

[Abstract] [PDF Full-Text (276 KB)] **IEEE CNF**

11 **Low power digital design in FPGAs: a study of pipeline architectures implemented in a FPGA using a low supply voltage to reduce power consumption**
*Garcia, A.; Burleson, W.; Danger, J.L.;*
Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on , Volume: 5 , 28-31 May 2000
Page(s): 561 -564 vol.5

[Abstract] [PDF Full-Text (400 KB)] **IEEE CNF**

12 **A generic systolic processor for real time grayscale morphology**
*Deforges, O.; Normand, N.;*
Acoustics, Speech, and Signal Processing, 2000. ICASSP '00. Proceedings. 2000 International Conference on , Volume: 6 , 5-9 June 2000
Page(s): 3331 -3334 vol.6

[Abstract] [PDF Full-Text (300 KB)] **IEEE CNF**

13 **Efficient 8-cycle DES implementation**
*Young Won Lim;*
ASICs, 2000. AP-ASIC 2000. Proceedings of the Second IEEE Asia Pacific Confer on , 28-30 Aug. 2000
Page(s): 175 -178

[Abstract] [PDF Full-Text (352 KB)] **IEEE CNF**

14 **Security and performance optimization of a new DES data encryption**
*Verbauwhede, I.; Hoornaert, F.; Vandewalle, J.; De Man, H.J.;*
Solid-State Circuits, IEEE Journal of , Volume: 23 Issue: 3 , June 1988
Page(s): 647 -656

[Abstract] [PDF Full-Text (960 KB)] **IEEE JNL**

15 **Performance analysis of a pipelined backpropagation parallel algorit**
*Petrowski, A.; Dreyfus, G.; Girault, C.;*
Neural Networks, IEEE Transactions on , Volume: 4 Issue: 6 , Nov. 1993
Page(s): 970 -981

[Abstract] [PDF Full-Text (1128 KB)] **IEEE JNL**

Home | Log-out | Journals | Conference Proceedings | Standards | Search by Author | Basic Search | Advanced Search
Join IEEE | Web Account | New this week | OPAC Linking Information | Your Feedback | Technical Support | Email Alerting
No Robots Please | Release Notes | IEEE Online Publications | Help | FAQ| Terms | Back to Top

Your search matched **20** of **988420** documents.

A maximum of **20** results are displayed, **15** to a page, sorted by **Relevance** in **descending** order.
You may refine your search by editing the current search expression or entering a new one the text box.
Then click **Search Again**.

permutation<and>substitution Search Again

**Results:**
Journal or Magazine = **JNL** Conference = **CNF** Standard = **STD**

1 **A private key cryptosystem based upon enforced random substitution scheme**
*Yeh, Y.-S.; Wu, T.-C.; Chang, C.-C.; Chang, D.;*
Security Technology, 1991. Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on , 1-3 Oct. 1991
Page(s): 319 -324

[Abstract] [PDF Full-Text (312 KB)] **IEEE CNF**

2 **A new criterion for the design of 8×8 S-boxes in private-key ciphers**
*Jianhong Xu; Heys, H.M.;*
Electrical and Computer Engineering, 1997. IEEE 1997 Canadian Conference on
Volume: 1 , 25-28 May 1997
Page(s): 322 -325 vol.1

[Abstract] [PDF Full-Text (316 KB)] **IEEE CNF**

3 **Differential-like cryptanalysis of a class of substitution-permutation networks**
*Chen, Z.G.; Youssef, A.M.; Tavares, S.E.;*
Electrical and Computer Engineering, 1998. IEEE Canadian Conference on , Vol 1 , 24-28 May 1998
Page(s): 433 -436 vol.1

[Abstract] [PDF Full-Text (300 KB)] **IEEE CNF**

4 **Provable security of substitution-permutation encryption networks a**

**linear cryptanalysis**
*Keliher, L.; Meijer, H.; Tavares, S.;*
Electrical and Computer Engineering, 2000 Canadian Conference on , Volume: 10 March 2000
Page(s): 37 -42 vol.1

[Abstract] [PDF Full-Text (472 KB)] **IEEE CNF**

5 **On the cryptanalysis of rotor machines and substitution - permutatio networks**
*Andelman, D.; Reeds, J.;*
Information Theory, IEEE Transactions on , Volume: 28 Issue: 4 , Jul 1982
Page(s): 578 -584

[Abstract] [PDF Full-Text (1128 KB)] **IEEE JNL**

6 **A differential cryptanalysis of tree-structured substitution-permutati networks**
*O'Connor, L.;*
Computers, IEEE Transactions on , Volume: 44 Issue: 9 , Sept. 1995
Page(s): 1150 -1152

[Abstract] [PDF Full-Text (272 KB)] **IEEE JNL**

7 **Avalanche characteristics of substitution-permutation encryption net**

*Heys, H.M.; Tavares, S.E.;*
Computers, IEEE Transactions on , Volume: 44 Issue: 9 , Sept. 1995
Page(s): 1131 -1139

[Abstract] [PDF Full-Text (800 KB)] **IEEE JNL**

8 **Improved numerical stability of sparse matrix reduction method**
*Bratkovic, F.;*
Circuits and Systems, 1988., IEEE International Symposium on , 7-9 June 1988
Page(s): 631 -634 vol.1

[Abstract] [PDF Full-Text (208 KB)] **IEEE CNF**

9 **New algorithms for static and dynamic sensitization of paths in timin**

**analysis**
*Abdallah, N.; Kiani, P.; Hajjar, A.;*
System Theory, 1994., Proceedings of the 26th Southeastern Symposium on , 2 March 1994
Page(s): 385 -389

[Abstract] [PDF Full-Text (340 KB)] **IEEE CNF**

---

10 **A new approach to abstract syntax involving binders**
*Gabbay, M.; Pitts, A.;*
Logic in Computer Science, 1999. Proceedings. 14th Symposium on , 2-5 July 1
Page(s): 214 -224

[Abstract] [PDF Full-Text (212 KB)] **IEEE CNF**

---

11 **A block cipher technique for security of data and computer networks**
*Rahouma, K.H.;*
Internet Workshop, 1999. IWS 99 , 18-20 Feb. 1999
Page(s): 25 -31

[Abstract] [PDF Full-Text (596 KB)] **IEEE CNF**

---

12 **Known plaintext cryptanalysis of tree-structured block ciphers**
*Heys, H.M.; Tavares, S.E.;*
Electronics Letters , Volume: 31 Issue: 10 , 11 May 1995
Page(s): 784 -785

[Abstract] [PDF Full-Text (184 KB)] **IEE JNL**

---

13 **Secure and fast encryption using chaotic Kolmogorov flows**
*Scharinger, J.;*
Information Theory Workshop, 1998 , 22-26 June 1998
Page(s): 124 -125

[Abstract] [PDF Full-Text (248 KB)] **IEEE CNF**

---

14 **Custom hardware for high performance and high security digital dat ciphering**
*Noras, J.M.;*
Security and Detection, 1995., European Convention on , 16-18 May 1995

Page(s): 128 -132

[Abstract] [PDF Full-Text (472 KB)] **IEE CNF**

15 **Sparse matrix computations on an FFP machine**
*Smith, B.T.; Singh, R.K.; Mago, G.A.;*
Frontiers of Massively Parallel Computation, 1988. Proceedings., 2nd Symposium the Frontiers of , 10-12 Oct. 1988
Page(s): 215 -218

[Abstract] [PDF Full-Text (344 KB)] **IEEE CNF**

1 2 [Next]

Home | Log-out | Journals | Conference Proceedings | Standards | Search by Author | Basic Search | Advanced Search
Join IEEE | Web Account | New this week | OPAC Linking Information | Your Feedback | Technical Support | Email Alerting
No Robots Please | Release Notes | IEEE Online Publications | Help | FAQ| Terms | Back to Top

Your search matched **20** of **988420** documents.

A maximum of **20** results are displayed, **15** to a page, sorted by **Relevance** in **descending** order.
You may refine your search by editing the current search expression or entering a new one the text box.
Then click **Search Again**.

permutation<and>substitution Search Again

**Results:**
Journal or Magazine = **JNL** Conference = **CNF** Standard = **STD**

16 **A state machine approach to reliable distributed systems**
*Lim, A.S.; Friedberg, S.A.;*
Reliable Distributed Systems, 1992. Proceedings., 11th Symposium on , 5-7 Oc

Page(s): 204 -212

[Abstract] [PDF Full-Text (844 KB)] **IEEE CNF**

17 **Reducing inconsistency in integrating data from different sources**
*Lujan-Mora, S.; Palomar, M.;*
Database Engineering & Applications, 2001 International Symposium on. , 16-1 2001
Page(s): 209 -218

[Abstract] [PDF Full-Text (740 KB)] **IEEE CNF**

18 **Hardware implementation for fast convolution with a PN code using programmable gate array**
*Alaqeeli, A.; Starzyk, J.;*
Southeastern Symposium on System Theory, 2001. Proceedings of the 33rd , 1 March 2001
Page(s): 197 -201

[Abstract] [PDF Full-Text (368 KB)] **IEEE CNF**

19 **Logical manipulations and design of tributary networks in the arithm spectral domain**

*Chang, C.-H.; Falkowski, B.J.;*
Computers and Digital Techniques, IEE Proceedings- , Volume: 145 Issue: 5 , S 1998
Page(s): 347 -356

[Abstract] [PDF Full-Text (864 KB)] **IEE JNL**

---

20 **Cryptanalysis of tree-structured substitution-permutation networks**
*Heys, H.M.; Tavares, S.E.;*
Electronics Letters , Volume: 29 Issue: 1 , 7 Jan 1993
Page(s): 40

[Abstract] [PDF Full-Text (180 KB)] **IEE JNL**

---

[Prev] 1 2

Home | Log-out | Journals | Conference Proceedings | Standards | Search by Author | Basic Search | Advanced Search
Join IEEE | Web Account | New this week | OPAC Linking Information | Your Feedback | Technical Support | Email Alerting
No Robots Please | Release Notes | IEEE Online Publications | Help | FAQ| Terms | Back to Top